

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/838,979	04/19/2001	Peter V. Radatti	16-00	1266

7590 09/23/2004
CyberSoft, Inc.
1508 Butler Pike
Conshohocken, PA 19428

EXAMINER

KLIMACH, PAULA W

ART UNIT PAPER NUMBER

2135

DATE MAILED: 09/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/838,979	Applicant(s) RADATTI, PETER V.	
	Examiner Paula W Klimach	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 April 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 103

Claims 1-4 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jordan (2002/0073323 A1).

In reference to claim 1 and 6, Jordan discloses a system and method for detecting computer viruses that attempt to gain access to restricted computer (abstract). The method includes writing the results and scanning the results for the presence of proscribed code (page 3 paragraph 0028).

Although Jordan does not expressly disclose interpreting code, Jordan discloses an emulator that emulates the executable code (page 3 paragraph 0028).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the emulator to perform the function of the interpreter. One of ordinary skill in the art would have been motivated to do this because it is desirable that the malicious code is not executed and the interpreter and the emulator do not execute the code, instead they simulate the execution of the code.

In reference to claim 2, wherein the step of scanning further comprising a first scanning step for the presence of code of interest. Jordan discloses detecting modification of memory (page 3 paragraph 0027) and therefore code of interest.

In reference to claim 3, wherein the first scanning step for the presence of code of interest further comprises scanning for a file open command or a file modify command. Jordan discloses detecting modification of memory (page 3 paragraph 0027). Modifying a file will modify memory.

Art Unit: 2135

In reference to claim 4, wherein the step of scanning further comprising a second scanning step for the presence of proscribed code of interest. Jordan discloses detecting modification of memory (page 3 paragraph 0027), the access of memory includes accessing restricted computer system resources; this is the presence of proscribed code.

Claims 5, 7-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jordan as applied to claim 1, and 4 respectfully above, and further in view of Shieh et al (5,278,901).

In reference to claim 7, is rejected as in claim 1 a system and method for detecting computer viruses that attempt to gain access to restricted computer (abstract). The method includes interpreting code (emulator) that emulates the executable code (page 3 paragraph 0028), a reporter and a results evaluator (page 3 paragraph 0028), whereby the file is interpreted by the emulator and results generated those results sent to the evaluator (detector) that determines if malicious code is present and then the results are reported. However Jordan does not expressly disclose a pattern analyzer.

However Shieh discloses a pattern-oriented system and method of intrusion detection (column 4 lines 9-22). The patten-oriented system is used to detect virus propagation (xolumn 16 lines 31 to column 17 line 30); therefore the pattern analyzer reviews patterns for the presence of proscribed code.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add a pattern analyzer for detection for intrusion detection as in the system by Shieh in the system of Jordan. One of ordinary skill in the art would have been motivated to do

this because patterns are a simple way of defining deviation from the normal operation of the system.

In reference to claim 5, Jordan does not expressly disclose a system wherein the second scanning step for the presence of proscribed code of interest further comprises scanning for viral code or viral patterns.

However Shieh discloses a pattern-oriented system and method of intrusion detection (column 4 lines 9-22).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use pattern detection for intrusion detection as in the system by Shieh in the system of Jordan. One of ordinary skill in the art would have been motivated to do this because patterns are a simple way of defining deviation from the normal operation of the system..

In reference to claim 8, wherein the step of scanning further comprising a first scanning step for the presence of code of interest. Jordan discloses detecting modification of memory (page 3 paragraph 0027) and therefore code of interest.

In reference to claim 9, wherein the first scanning step for the presence of code of interest further comprises scanning for a file open command or a file modify command. Jordan discloses detecting modification of memory (page 3 paragraph 0027). Modifying a file will modify memory.

In reference to claims 10-12, Jordan does not expressly disclose the pattern analyzer further reviews said code for the presence of code of interest.

Shieh discloses the pattern analyzer reviews code for the presence of problems, or code of interest (column 4 line 60 to column 5 line 11).

Art Unit: 2135

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use pattern detection for code of interest as in the system by Shieh in the system of Jordan. One of ordinary skill in the art would have been motivated to do this because patterns are a simple way of defining deviation from the normal operation of the system.


Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

The 2100 Tech center will move to Carlyle in October 2004. The new telephone number for the receptionist is (571) 272-2100. The examiner's new telephone number will be (571) 272-3854.



KIM VU
PATENT EXAMINER
TECHNOLOGY CENTER 2100